REMARKS

Claims 1-38 are pending in this application. By this Amendment, the specification and claims 1, 5, 7, 20, 21, 24-26, 28 and 31-33 are amended. Claims 1, 5, 7, 20, 21, 24-26, 28 and 33 are amended to recite features supported in the specification, for example, at page 20, lines 5-23, and page 58, line 25 – page 60, line 7 and Fig. 20. Claims 21 and 25 are amended to more positively recite method steps. No new matter is added by any of these amendments.

Applicant appreciates the courtesies extended to Applicant's representative by Examiner Kim during the December 16, 17 and 20, 2004 telephone interviews.

Reconsideration based on the following remarks is respectfully requested.

I. Amendment Entry after Final Rejection

The foregoing amendments do not raise any new issues after Final Rejection. Therefore, entry of the amendments is proper under 37 CFR §1.116 because the amendments place the application in condition for allowance. Accordingly, Applicant respectfully requests entry of this Amendment.

II. Claims 1-38 Define Patentable Subject Matter

The Final Office Action rejects claims 1, 2, 5-10, 19 and 20 under 35 U.S.C. §103(a) over U.S. Patent 6,154,541 to Zhang in view of U.S. Patent 5,768,382 to Schneier *et al.* (identified in the Final Office Action as Walker, and hereinafter referenced as "Schneier '382") and U.S. Patent 6,625,295 to Wolfgang *et al.* (hereinafter "Wolfgang"). This rejection is respectfully traversed.

Zhang, Schneier '382 and Wolfgang, alone or in combination, do not teach or suggest a method for generating a one-way function dependent on a one-way function H and a unique value d for a user, including holding in memory a function generation unique value s by a right issuer for the user, creating a value generation unique value u in a unique value calculation unit from the function generation unique value s provided from the memory and the unique value d, the value generation unique value u being provided as a series of m values

where $u = (u_1,...u_m)$ to a token for the user, creating by a hash value calculation unit a one-way function value X(M) of a message M by applying the one-way function H to the value generation unique value u from the unique value calculation unit and the message M, where the one-way function value $X(M) = H(u_1 | M) | ... | H(u_m | M)$, issuing a capability χ from the right issuer to the user, the capability χ representing a right of the user in association with the message M, and verifying the user from a public key y and the capability χ by a right verifier, as recited in claim 1, and similarly recited for a device for generating one-way function values in claim 5.

Nor do Zhang, Schneier '382 and Wolfgang, alone or in combination, teach or suggest a proving device for performing processing based on a private key for a user dependent on a message M that includes means for inputting the message M, means for holding a value generation unique value u for the user, means for creating a one-way function value X(M) of the message M by applying a one-way function H to the value generation unique value u from the holding means and the message M, for performing processing based on the one-way function value X(M), means for issuing a capability χ from the right issuer to the user, the capability χ representing a right of the user in association with the message M; and means for verifying the user from a public key y and the capability χ, wherein the value generation unique value u is created from a function generation unique value s being held and provided by a right issuer and a unique value d for the user, the value generation unique value u being provided as a series of m values where $u = (u_1,...u_m)$ to a token for the user, and the one-way function value $X(M) = H(u_1 | M) | ... | H(u_m | M)$, as recited in claim 7, and similarly recited for an proving instrument issuing device for an instrument T in claim 20.

For example, the specification discloses various exemplary aspects of an authentication device to verify rights based on a message M provided to a user recipient (35) from a right issuer (33) receiving a capability χ. The user (35) is verified by a right verifier (37) having a public key y (page 58, line 25 – page 60, line 7 and Fig. 20). The specification

further discloses a calculation unit (4) for determining unique value u based on unique values d and s, and a hash value calculation unit (5) based on the calculated unique value u and the input message M, which a hash value X(M). A private key processing unit (8) receiving the hash value X(M) includes a response generation unit (10) that also receives a challenge c and produces a response r (page 18, line 12 – page 19, line 3, page 21, lines 8-17 and Figs. 1-3). The response generation unit (10) may also receive a random number k and output a commitment w (page 24, lines 16-26, page 28, lines 13-23, page 32, lines 9-15 and Figs. 4-6).

The specification further discloses, for example, a certificate verification unit (18) and a private key processing verification unit (19) that interacts with a proving instrument (page 34, line 22 – page 35, line 6 and Fig. 8). A hash value generator with inputs d and M enable a public key calculation unit (23) to pass a public key y to a certificate issuing unit (24) for a certificate C (page 42, lines 18-23 and Fig. 12). The public key y can be input to a private key processing verification unit (19) and communicate with a private key processing conversion unit (27), which receives an access ticket t (page 44, lines 15-26 and Fig. 13). The ticket t, calculated by a calculation unit (31) and issued by an issuing unit (32) may also update units (28, 29) to update the challenge c and the response r (page 45, lines 13-19 and Figs. 14-19).

To the contrary, Zhang discloses a cryptographic system that encrypts a ciphertext C by a key vector K_c. In particular, Zhang teaches loading data bits into a data register 41, resetting a code register 42, shifting bits by a shifter 43 and fed to a multiplier 45 (col. 14, lines 11-60 and Fig. 4 of Zhang). However, Zhang lacks teachings regarding the method steps for the input and calculation units or means recited in Applicant's claimed features. Such teachings are unrelated to the value generation and function generation unique values in conjunction with the value generation units and issuing units, as provided in Applicant's claims.

The Final Office Action admits on page 6 (paragraph 14) that Zhang does not disclose "the unique value s to be held by a center", but asserts that trusted third parties as institutions provide certified values used to seed an encryption key, such as by distribution of timestamps (col. 28, lines 11-15 of Schneier '382) and use of a time stamp as a seed value (col. 7, lines 49-52 of Wolfgang). Thus, the Final Office Action asserts that it would have been obvious for the unique value s to be held by a center and enable a key to be implemented thereby. Applicant respectfully disagrees and asserts that Applicant's claimed features are directed to creating a value generation unique value u based on the user's unique value d and the function generation unique value s, which is not taught or suggested by the applied references, alone or in combination. Moreover, there is no teaching or suggestion for issuing a capability χ to the user representing a right in association with the message M, as recited in claims 1, 5, 7 and 20.

Further, Schneier '382 discloses protocols for coding and encoding messages on game outcomes. In particular, Schneier '382 teaches a central computer 12 associated with game computers 14 operating game software 15 in memory 23. Schneier '382 further teaches encrypting an outcome message by a game computer 14 with a public-key/private-key pair to form an authentication outcome message (AOM), and accepting the AOM by the central computer 12 using signature verification and the public key (col. 5, lines 29-56, col. 10, lines 27-56 and Figs. 1A and 5 of Schneier '382). Although Schneier '382 discloses use of "tokens", these constitute physical computing devices, and thus their context differs from Applicant's claimed features as a tamper-resistant enclosure for a private key.

Also, Wolfgang discloses a method of signal authentication by applying a watermark. In particular, Wolfgang teaches a watermark 50 incorporated in an original image 52 by an algorithm 54 to produce a watermarked image 56 (col. 6, lines 33-37 and Fig. 2 of Wolfgang).

Further, there is no motivation to combine features related to the databit manipulation of Zhang with the game message encoding protocol of Schneier '382 and the signal watermarks of Wolfgang, nor has the Final Office Action established sufficient motivation for a *prima facie* case of obviousness. Even assuming that motivation to combine the applied references is established, the combination fails to teach or suggest Applicant's claimed features.

The Final Office Action further rejects claims 18, 21-30 and 33 under 35 U.S.C. §103(a) over Zhang in view of Schneier '382 and Wolfgang and further in view of *Cryptography and Network Security*, 2nd ed. by Stallings. The Final Office Action further rejects claims 3, 4 and 11-17 under 35 U.S.C. §103(a) over Zhang in view of Schneier '382 and Wolfgang and further in view of *Applied Cryptography*, 2nd ed. by Schneier *et al.* (hereinafter "Schneier *AC*"). The Final Office Action further rejects claims 31, 32 and 34-38 under 35 U.S.C. §103(a) over Zhang in view of Schneier '382, Wolfgang, Stallings and Schneier *AC*.

Zhang, Schneier '382 and Wolfgang, alone or in combination, also fail to teach or suggest an authentication method by which a right issuer issues rights to right recipients in association with a message M and a right verifier verifies the rights of the right recipients, including, *inter alia*, creating a value generation unique value u from a function generation unique value s being held and provided by a function generation unique value memory and a unique value d for a user corresponding to the right recipients, the value generation unique value u being provided as a series of m values where $u = (u_1,\ldots u_m)$ to a token for the user, calculating a one-way function value X(M) of the message M by a hash value generator by applying a one-way function H to the value generation unique value u and the message M, where the one-way function value $X(M) = H(u_1 \mid M) \mid \ldots \mid H(u_m \mid M)$, performing processing by a private key processing unit based on the one-way function value X(M), and verifying the

processing by a private key processing verification unit based on the one-way function value X(M) of the right recipients with a public key y, as recited in claims 21 and 26.

The Final Office Action admits on page 9 (paragraph 22) that Zhang does not teach or suggest "the message M including the use conditions of the message by the method", but asserts that Stallings teaches use conditions for X.509 certificates. The Final Office Action further asserts that motivation for combining these teachings enables distribution of several types of messages. Applicant respectfully disagrees and asserts that employing use conditions for a certificate C enables proving a public key y, whereas Applicant's claimed features recite that the message M provides an input for calculating the one-way function value X(M) used for private key processing. Therefore, the use conditions for the message M cannot be considered analogous to such techniques applied to the certificate C.

The Final Office Action admits on page 12 (paragraph 31) that Zhang does not teach "an encryption function with a symmetric key as the scrambling operation", but that Schneier *AC* teaches scrambling techniques, and that applying these teachings to Zhang would be obvious. Applicant respectfully disagrees, and asserts that Applicant's claims 11-14 further recite inputting a challenge c and calculating a response r from the challenge c and the one-way function value X(M). Thus, Applicant submits that scrambling with a symmetric key has no relationship with any of the steps of producing a random number k, calculating a commitment w from the random number k, and calculating a response r from an input challenge c, a one-way function value X(M), the random number k and the commitment w, as recited in Applicant's claimed features. Nor does the symmetric key scrambling render obvious multiplications and power operations of multiplicative groups, as recited in Applicant's claims.

The Final Office Action admits on page 14 (paragraph 35) that Zhang fails to teach "combining two values" as bit concatenation, but asserts that such operations are typical when values are of differing sizes, such as in the data encryption standard (DES). Applicant

respectfully disagrees, and asserts that Zhang instead provides k number of sections of a key set used in PPKS to control a wrinkling effect, that ranges of numbers based on points I facilitate random number seeding, as well as generating fuzzy residues (col. 15, lines 29-67 of Zhang). However, such teachings are not related to series for the value generation unique value u, as recited in Applicant's claimed features. Moreover, Applicant asserts that by applying encryption to game machine accounting, Zhang teaches away from bit concatenation as an unnecessary and computationally demanding adornment.

The Final Office Action admits on page 15 (paragraph 36) that Zhang does not disclose "using the access ticket to update values used in authentication", but asserts that such difference or quotient teachings would be obvious constructions to show equality or inequality of two values. Applicant respectfully disagrees, and asserts that updating the challenge c and/or the response r is unrelated to the necessity of showing equivalence between values. Moreover, Zhang lacks any teaching or suggestion to update values or to use access tickets in authentication.

Stallings and Schneier *AP* do not compensate for the deficiencies of Zhang, Schneier '382 and Wolfgang outlined above for claims 1 and 7. Nor does Stallings teach, disclose or suggest the additional features recited in claims 18, 21-30 and 33. Also, Schneier *AC* fails to teach, disclose or suggest the additional features recited in claims 3, 4 and 11-17. Further, Stallings and Schneier *AC* do not teach, disclose or suggest the additional features recited in claims 31, 32 and 34-38.

Instead, Stallings discloses certificate authentication. In particular, Stallings teaches the X.509 scheme procedures. The X.509 protocol associates a user with a public-key certificate created by a trusted certified authority, which signs the certificate with a secret key (§11.2 of Stallings). In contrast, Applicant's claimed features are directed to verifying the processing by a private key processing verification unit based on the one-way function value

X(M), as recited in claim 21, or for issuing a capability χ to the user representing a right in association with the message M, as recited in claim 24.

In addition, Schneier *AC* discloses encryption and decryption protocols. In particular, Schneier *AC* teaches algorithm complexity comparison and describes the DES block cipher, using permutations and substitutions of keys divided by halves (§§11.2, 12.2 of Schneier *AC*). Such teachings do not compensate for the deficiency regarding calculating the one-way function value X(M) based on the message M or for the subdivision into series of the value generation unique value u, as recited in Applicant's claimed features.

Further, there is no motivation to combine features related to the databit manipulation of Zhang with the game message encoding protocol of Schneier '382, the signal watermarks of Wolfgang, the authentication procedures of Stallings and the cryptographic protocols of Schneier *AC*, nor has the Final Office Action established sufficient motivation for a *prima facie* case of obviousness. Even assuming that motivation to combine the applied references is established, the combinations fail to teach or suggest Applicant's claimed features.

A *prima facie* case of obviousness for a §103 rejection requires satisfaction of three basic criteria: 1) there must be some suggestion or motivation either in the references or knowledge generally available to modify the references or combine reference teachings, 2) a reasonable expectation of success, and 3) the references must teach or suggest all the claim limitations (MPEP §706.02(j)). Applicant asserts that the Final Office Action fails to satisfy these requirements with Zhang, Schneier '382, Wolfgang, Stallings and/or Schneier *AC*.

For at least these reasons, Applicant respectfully asserts that the independent claims are now patentable over the applied references. The dependent claims are likewise patentable over the applied references for at least the reasons discussed as well as for the additional features they recite. Consequently, all the claims are in condition for allowance. Thus, Applicant respectfully requests that the rejections under 35 U.S.C. §103 be withdrawn.

III. Conclusion

In view of the foregoing amendments and remarks, Applicant respectfully submits that this application is in condition for allowance. Favorable reconsideration and prompt allowance are earnestly solicited.

Should the Examiner believe that anything further is desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact Applicant's undersigned representative at the telephone number listed below.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Gerhard W. Thielman
Registration No. 43,186

JAO:GWT/gwt

Date: January 26, 2005

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461